Neliöjäännösjärjestelmä ja sen käyttö salauksessa

LuK-tutkielma
Tuomas Peltoketo
2562465
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2021

Sisältö

Johdanto

Tässä tukielmassa tarkastellaan neliöjäännösjärjestelmää ja sen käyttöä salauksessa. Aluksi tutkitaan itse neliöjäännösjärjestelmää ja siihen liittyviä laskutoimituksia. Neliöjäännöksien laskeminen ilman apukeinoja on kuitenkin erittäin hidasta, sillä joudutaan laskemaan $\frac{p-1}{2}$ laskutoimitusta, että saadaan selville kaikki neliöjäännökset. Tämä ei ole pienillä p:n arvoilla ongelma, mutta kun käsitellään isompia lukuja tarvitaan tehokkaampia keinoja.

Tutkielmassa esitellään myös neliöjäännöksen käänteisyys ja Jacobin symboli, joita käyttämällä saadaan vähennettyä tarvittavia laskutoimituksia huomattavasti. Lopuksi tutkitaan Goldwasser-Micalin satunnaistettua salausjärjestelmää ja Rabinin allekirjoitusjärjestelmää, joissa käytetään hyödyksi neliöjäännösjärjestelmää ja aikaisemmin määriteltyjä lauseita. Pääasiallisena lähteenä on käytetty teoksen Jeffrey Hoffstein, Jill Pipher ja Joseph H. Silverman, An Introduction to Mathematical Cryptography sivuja 165-187 [1].

1 Neliöjäännösjärjestelmä ja sen laskutoimitukset

Kohdat 1.4, 1.5 ja 2.1 ovat omia huomioita ja Lauseessa 1.9 ollaan käytetty lähdettä [2].

1.1 Neliöjäännösjärjestelmä

Neliöjäännösjärjestelmässä tutkitaan lukuja, jotka saadaan, kun jokin kokonaisluku korotetaan toiseen potenssiin ja otetaan jakojäännös luvun p kanssa, jossa p on pariton alkuluku. Tästä saadaan seuraava määritelmä.

Määritelmä 1.1. Olkoon p pariton alkuluku ja a kokonaisluku siten, että $p \nmid a$. Luku a on eräs *neliöjäännös* mod p, jos on olemassa luku c siten, että $c^2 \equiv a \mod p$. Jos lukua c ei ole olemassa, luku a on *epäneliöjäännös* mod p.

Luvun neliöjäännöllisyyden voi tutkia laskemalla kaikkien lukujen neliöt luvusta 1 lukuun $\frac{p-1}{2}$ asti, että saadaan selville onko lukua c^2 olemassa. Arvoista $1, 2, ...p$ tarvitsee tutkia vain puolet, sillä $a^2 \equiv (-a)^2 \mod p$.

Esimerkki 1.2. Ovatko luvut 11 ja 41 neliöjäännöksiä mod 53?

Muodostetaan taulukko, josta nähdään kaikki neliöjäännökset.

$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 9$	$4^2 \equiv 16$	$5^2 \equiv 25$	$6^2 \equiv 36$	$7^2 \equiv 49$
$8^2 \equiv 11$	$9^2 \equiv 28$	$10^2 \equiv 47$	$11^2 \equiv 15$	$12^2 \equiv 38$	$13^2 \equiv 10$	$14^2 \equiv 37$
$15^2 \equiv 13$	$16^2 \equiv 44$	$17^2 \equiv 24$	$18^2 \equiv 6$	$19^2 \equiv 43$	$20^2 \equiv 29$	$21^2 \equiv 17$
$22^2 \equiv 7$	$23^2 \equiv 52$	$24^2 \equiv 46$	$25^2 \equiv 42$	$26^2 \equiv 40$		

Saadusta neliöjäännöstaulukosta nähdään, että 11 on eräs neliöjäännös mod 53, kun taas 41 on eräs epäneliöjäännös mod 53. Taulukosta huomataan myös, että kyseinen tapa ei ole kovin tehokas neliöjäännöksien määrittämiseen ja etsimiseen, sillä se vaatii enimmillään $\frac{p-1}{2}$ laskutoimitusta.

1.2 Tulo neliöjäännösjärjestelmässä

Seuraava lause käsittelee neliöjäännöksien ja epäneliöjäännöksien kertolaskuja.

Lause 1.3. *Olkoon p pariton alkuluku.*
1. Kahden neliöjäännöksen tulo mod p on aina neliöjäännös mod p.
2. Neliöjäännöksen ja epäneliöjäännöksen tulo mod p on epäneliöjäännös mod p.
3. Kahden epäneliöjäännöksen tulo mod p on neliöjäännös mod p.

Todistus. Jos p on pariton alkuluku, niin on olemassa primitiivijuuri g, joka generoi jäännösluokan *mod* p. Arvot $1, g, g^2, ..., g^{p-2}$ ovat siis eri suuruisia ja muodostavat jäännösluokan *mod* p kaikki alkiot.

Kun g:n potenssi m on parillinen $m = 2k, \quad k \in \mathbb{Z}$, niin $g^m \equiv g^k g^k \equiv \left(g^k\right)^2 \equiv a \mod p$. Määritelmän 1.1 perusteella a on neliöjäännös eli, jos g:n potenssi m on parillinen, niin tulos on neliöjäännös.

Olkoon g:n potenssi pariton eli $m = 2k + 1$. Oletetaan, että on olemassa neliöjäännös c siten, että $c^2 = g^{2k+1} \bmod p$.

Fermat'n pienen lauseen mukaan $c^{p-1} \equiv 1 \bmod p$.

$$1 \equiv c^{p-1} \equiv \left(c^2\right)^{\frac{p-1}{2}} \bmod p.$$

Alun oletuksien $c^2 \equiv g^m \bmod p$ ja $m = 2k + 1$ mukaan voidaan merkitä

$$\left(c^2\right)^{\frac{p-1}{2}} \equiv \left(g^m\right)^{\frac{p-1}{2}} \equiv \left(g^{2k+1}\right)^{\frac{p-1}{2}} \equiv g^{k(p-1)} \cdot g^{\frac{p-1}{2}} \bmod p.$$

Fermat'n pienen lauseen mukaan:

$$g^{k(p-1)} \equiv \left(g^{p-1}\right)^k \equiv 1^k \equiv 1 \bmod p.$$

Tästä seuraa, että:

$$g^{k(p-1)} \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Tämä on ristiriidassa oletuksen kanssa, että primitiivialkio g:n potenssit $1, 2..., (p-1)$ ovat erisuuruisia kuin arvo 1.

Nyt ollaan todistettu, että:

$$g^m = \begin{cases} \text{neliöjäännös}, & jos\ m = 2k,\ k \in\ \mathbb{Z}, \\ \text{epäneliöjäännös}, & jos\ m = 2k+1,\ k \in\ \mathbb{Z}. \end{cases}$$

1. Olkoon a ja b neliöjäännöksiä. Esitetään luvut muodossa $a \equiv g^{2i}\ \ mod\ p$ ja $b \equiv g^{2j}\ \ mod\ p$. Nyt luvulla $ab \equiv g^{2(i+j)}\ \ mod\ p$ on parillinen eksponentti joten ab on neliöjäännös $mod\ p$.

2. Olkoon c neliöjäännös ja d epäneliöjäännös. Merkitään $c \equiv g^{2i}\ \ mod\ p$ ja $d \equiv g^{2j+1}\ \ mod\ p$. Nyt $cd \equiv g^{2(i+j)+1}\ \ mod\ p$. Saatu potenssi on pariton joten cd on epäneliöjäännös $mod\ p$.

3. Olkoon e ja f epäneliöjäännöksiä. Merkitään $e \equiv g^{2i+1}\ \ mod\ p$ ja $f \equiv g^{2j+1}\ \ mod\ p$. Nyt $fe \equiv g^{2(i+j+1)}\ \ mod\ p$. Saatu potenssi on parillinen joten ef on neliöjäännös $mod\ p$. □

Lause 1.4. *Olkoon a neliöjäännös mod p, jossa p on pariton alkuluku. Tällöin on olemassa yksikäsitteinen kokonaisluku r välillä $0 < r \leqslant \frac{p-1}{2}$, jolle pitää paikkansa, että $r^2 \equiv a\ mod\ p$.*

Todistus. Koska p on pariton alkuluku, niin on olemassa yksikäsitteinen generoijaalkio g, joka generoi koko jäännösluokan mod p. Tehdään vastaoletus, että r ei ole yksikäsitteinen välillä $0 < r \leqslant \frac{p-1}{2}$. On siis olemassa $r^2 \equiv a \bmod p$ ja $h^2 \equiv a \bmod p$, jossa $0 < r \leqslant \frac{p-1}{2}$ ja $0 < h \leqslant \frac{p-1}{2}$ sekä $r \neq h$. Merkitään $g^{2n} \equiv r^2 \equiv a \bmod p$ ja $g^{2m} \equiv h^2 \equiv a \bmod p$. Tästä seuraa, että $g^{2n} \equiv g^{2m} \bmod p$, $2n \equiv 2m \bmod p-1$ ja $n \equiv m \bmod \frac{p-1}{2}$. Tällöin

$$r^2 \equiv g^{2n} \equiv h^2 \equiv g^{2m}.$$

Saadusta tuloksesta huomataan, että

$$h \equiv r \bmod p \text{ tai } h \equiv -r \bmod p.$$

Tilanne $h \equiv r \bmod p$ tuottaisi heti ristiriidan alun oletuksen perusteella mutta toisaalta, jos $h \equiv -r \bmod p$, niin tämä tuottaa ristiriidan, koska luvun h pitää olla välillä $0 < h \leqslant \frac{p-1}{2}$. □

Seuraus 1.5. *Jokaisessa jäännösluokassa mod p, jossa p on pariton alkuluku on olemassa* $\frac{p-1}{2}$ *neliöjäännöstä ja* $\frac{p-1}{2}$ *epäneliöjäännöstä. Tästä seuraa, että satunnaisesti valittu kokonaisluku, joka ei ole jaollinen p:llä on* 50% *todennäköisyydellä neliöjäännös mod p ja on* 50% *todennäköisyydellä epäneliöjäännös mod p.*

Esimerkki 1.6. Esimerkin 1.2 luvut 11 ja 41 saadaan laskettua primitiivialkion $g = 2$ avulla seuraavasti: $2^6 \equiv 11 \mod 53$ ja $2^{45} \equiv 41 \mod 53$. Nyt luvun 2 potenssi 6 on selvästi parillinen eli 11 on eräs neliöjäännös ja luvun 2 potenssi 45 on pariton, joten 41 on epäneliöjäännös.

Lauseen 1.3 perusteella huomataan, että neliöjäännöksien (NJ) ja epäneliöjäännöksien (EJ) tuloilla on samat ominaisuudet kuin lukujen 1 ja -1 tuloilla:
$NJ * NJ = NJ, \quad NJ * EJ = EJ, \quad EJ * EJ = NJ.$

Koska neliöjäännös ja epäneliöjäännös omistavat tulossa samat ominaisuudet kuin luvut 1 ja -1, voidaan antaa seuraavan määritelmän mukaisesti neliöjäännökselle arvo 1 ja epäneliöjäännökselle arvo -1.

Määritelmä 1.7. Olkoon p pariton alkuluku. Tällöin kokonaisluvun a *Legendren symboli* luvun p suhteen määräytyy seuraavasti:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } a \text{ on neliöjäännös mod } p, \\ -1, & \text{jos } a \text{ on epäeliöjäännös mod } p, \\ 0, & \text{jos } p \text{ jakaa luvun } a. \end{cases}$$

Jakolaskun ja Legendren symbolin laskutoimitukset muistuttavat merkinnöiltään toisiaan, mutta eivät ole samoja. Tässä tutkielmassa merkitään Legendren symbolia $\left(\frac{\blacksquare}{\blacksquare}\right)$.

Neliöjäänöksien ja epäneliöjäännöksien tulo voidaan kuvata seuraavasti Legendren symbolin avulla:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Tämän lisäksi:

$$\text{jos} \quad a \equiv b \mod p, \quad \text{niin} \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Esimerkki 1.8. Onko luku 441 neliöjäännös mod 521?
Edellisen lauseen nojalla voidaan jakaa luku 441 tekijöihin $441 = 9 \cdot 49$, jolloin

$$\left(\frac{441}{521}\right) = \left(\frac{9}{521}\right)\left(\frac{49}{521}\right).$$

Koska luvut $3^2 = 9$ ja $7^2 = 49$ ovat neliöjäännöksiä mod 521, niin niille voi antaa Legendren symbolin arvon 1, joten

$$\left(\frac{9}{521}\right)\left(\frac{49}{521}\right) = 1 \cdot 1 = 1.$$

Koska luvun 441 Legendren symboli on 1 se on neliöjäännös mod 521.

Lause 1.9. ***Eulerin kriteria*** *Olkoon p pariton alkuluku ja luku a positiivinen kokonaisluku. Tästä seuraa:*

$$a^{\frac{p-1}{2}} = \begin{cases} 1, & \textit{jos } a \textit{ on neliöjäännös mod } p, \\ -1, & \textit{jos } a \textit{ ei ole neliöjäännös mod } p. \end{cases}$$

Todistus. Koska p on pariton alkuluku, niin on olemassa yksikäsitteinen generoija-alkio g. Lauseen 1.3 todistuksessa huomattiin, että generoija-alkion parilliset potenssit ovat neliöjäännöksiä ja parittomat potenssit epäneliöjäännöksiä. Tämä mahdollistaa sen, että voidaan tutkia tilanteet, joissa g:llä on parilliset ja parittomat potenssit.

1. Kun g:n potenssi on parillinen, niin:

$$\left(g^{2n}\right)^{\frac{p-1}{2}} = g^{n(p-1)} = \left(g^{(p-1)}\right)^n = 1^n = 1.$$

2. Kun g:n potenssi on pariton, niin:

$$\left(g^{2m+1}\right)^{\frac{p-1}{2}} = g^{m(p-1)} g^{\frac{p-1}{2}} = 1^m \cdot (-1) = -1.$$

□

Esimerkki 1.10. Luku 2 on neliöjäännös mod 7, sillä $2^3 \equiv 8 \equiv 1 \bmod 7$ tämän lisäksi luku 5 on epäneliöjäännös mod 7, sillä $5^3 \equiv 125 \equiv 6 \equiv -1 \bmod 7$.

1.3 Neliöjäännöksen käänteisyys

Aikaisempien lauseiden perusteella luvun neliöjäännöksen tutkiminen onnistuu ilman taulukon luomista vain, jos luvun voi jakaa tekijöihin, jotka ovat selvästi neliöjäännöksiä. Fermat'n pienen lauseen johdosta käytettäessäkin tarvittavien laskutoimitusten määrä on liian iso, että sitä voitaisiin käyttää esimerkiksi salausmenetelmissä.

Seuraava lause antaa tehokkaampia välineitä luvun neliöjäännöllisyyden tutkimiseen.

Lause 1.11. ***Neliöjäännöksen käänteisyys*** *Parittomien alkulukujen p ja q Legendren symboli voidaan määritellä seuraavasti:*

1. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & jos\ p \equiv 1 \mod 4, \\ -1, & jos\ p \equiv 3 \mod 4. \end{cases}$

2. $\left(\frac{2}{p}\right) = \begin{cases} 1, & jos\ p \equiv 1 \ tai\ p \equiv 7 \mod 8, \\ -1, & jos\ p \equiv 3 \ tai\ p \equiv 5 \mod 8. \end{cases}$

3. $\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & jos\ p \equiv 1 \mod 4 \ tai\ q \equiv 1 \mod 4, \\ -\left(\frac{q}{p}\right), & jos\ p \equiv 3 \mod 4 \ ja\ q \equiv 3 \mod 4. \end{cases}$

Todistus. Sivuutetaan.

□

Vaikka edellistä lausetta ei todisteta, on hyvä tutkia hieman tarkemmin, mitä kyseinen lause tarkoittaa ja miten se nopeuttaa neliöjäännöllisyyden tutkimista.

Kokonaislukujen p ja q jakojäännökset eivät voi olla parillisia parillisessa kongruenttiluokassa, sillä siitä seuraisi, että ne olisivat jaollisia kahdella, joka olisi ristiriidassa p:n ja q:n alkuluvullisuuden suhteen. Tästä seuraa, että kohdat 1, 2 ja 3 käsittelevät kaikki mahdolliset jäännösluokkien tilanteet.

Nimi neliöjäännöksen käänteisyys tulee ominaisuudesta 3. Sen avulla voidaan kääntää neliöjäännöllisyyttä kunnes päästään joko ominaisuuksiin 1 tai 2 tai lukuun, josta selvästi nähdään, että se on neliöjäännös.

Jotta voidaan käyttää neliöjäännöksen käänteisyyttä, niin pitää tietää, että luvut p ja q ovat alkulukuja. Isoilla p:n ja q:n arvoilla neliöjäännöksen käänteisyyden käyttö ei siis ole tehokasta.

Esimerkki 1.12. Onko luku -422 neliöjäännös mod 433?
Jaetaan luku -422 tekijöihin seuraavasti $-422 = -1 \cdot 2 \cdot 211$, jolloin

$$\left(\frac{-422}{433}\right) = \left(\frac{-1}{433}\right)\left(\frac{2}{433}\right)\left(\frac{211}{433}\right).$$

Koska $433 \equiv 3 \bmod 4$ ja mod 8, niin neliöjäännöksen käänteisyyden kohtien 1 ja 2 mukaan Legendren symboli luvuille -1 ja 2 on arvo 1, joten

$$\left(\frac{-1}{433}\right)\left(\frac{2}{433}\right)\left(\frac{211}{433}\right) = 1 \cdot 1 \cdot \left(\frac{211}{433}\right) = \left(\frac{211}{433}\right).$$

Koska $11 \equiv 3 \bmod 4$ ja $211 \equiv 3 \bmod 4$, niin neliöjäännöksen käänteisyyden kohdan 3 mukaan voidaan kääntää neliöjäännöllisyys, jolloin saadaan

$$\left(\frac{211}{433}\right) = \left(\frac{11}{211}\right) = -\left(\frac{211}{11}\right).$$

Koska $11 \equiv 3 \bmod 8$, niin luku 2 saa legendren symbolin arvon -1 mod 433, niin

$$-\left(\frac{211}{11}\right) = -\left(\frac{2}{11}\right) = -(-1) = 1.$$

Koska luvun -422 Legendren symboli on 1 mod 433, niin se on neliöjäännös mod 433.

Määritelmä 1.13. Olkoon luvut a ja b kokonaislukuja, joista b on pariton ja positiivinen. Tehdään b:lle alkulukuesitys seuraavasti:

$$b = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n},\ p \in P \text{ ja } e_n \in \mathbb{Z}\ \forall\ n \in \mathbb{Z}.$$

Kokonaisluvun a *Jacobin symboli* mod b suhteen määritellään seuraavasti:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\left(\frac{a}{p_3}\right)^{e_3}\cdots\left(\frac{a}{p_n}\right)^{e_n}.$$

Legendren symboli vaatii, että b ja a ovat alkulukuja. Jacobin symboli on siis yleistys, jolla voidaan jakaa b alkulukutekijöihin ja tutkia a:n neliöjäännöllisyyttä näiden tekijöiden suhteen.

Esimerkki 1.14. Onko luku 17 neliöjäännös mod 315?
Jaetaan luku 315 tekijöihin Jacobin symbolin mukaan $315 = 3^2 \cdot 5 \cdot 7$, jolloin

$$\left(\frac{17}{315}\right) = \left(\frac{17}{3}\right)^2 \left(\frac{17}{5}\right)\left(\frac{17}{7}\right) = \left(\frac{2}{3}\right)^2 \left(\frac{2}{5}\right)\left(\frac{3}{7}\right).$$

Neliöjäännöllisyyden käänteisyyden mukaan, koska $5 \equiv 5 \bmod 8$, niin luku 2 saa Jacobin symbolin arvon -1 ja, koska $7 \equiv 3 \bmod 4$, niin jäljelle jäänyt neliöjäännöllisyys voidaan kääntää ja muuttaa negatiiviseksi, jolloin

$$\left(\frac{2}{3}\right)^2 \left(\frac{2}{5}\right)\left(\frac{3}{7}\right) = 1 \cdot (-1) \cdot \left(-\frac{7}{3}\right) = 1 \cdot (-1) \cdot \left(-\frac{1}{3}\right) = 1 \cdot (-1) \cdot (-1) = 1.$$

Koska luvun 17 Jacobin symboli on 1, niin se on neliöjäännös mod 315.

Esimerkissä 1.12 ja Jacobin symbolia käytettäessä tarvitaan silti käsiteltävien lukujen tekijöihin jakoa. Tämä ei ole ongelma pienillä luvuilla, mutta isommille luvuille kyseiset tavat eivät ole tehokkaita.

Lause 1.15. *Olkoon luvut a_1, a_2, b_1 ja b_2 kokonaislukuja, joista b_1 ja b_2 ovat positiivisia ja parittomia. Jacobin symbolille määritellään samat kertolaskun ja yhtäsuuruuden ominaisuudet kuten Legendren symbolille.*

1.
$$\left(\frac{a_1 a_2}{b_1}\right) = \left(\frac{a_1}{b_1}\right)\left(\frac{a_2}{b_1}\right) \quad ja \quad \left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

2.
$$Jos \quad a_1 \equiv a_2 \ mod\ b_1, \quad niin \quad \left(\frac{a_1}{b_1}\right) = \left(\frac{a_2}{b_1}\right).$$

Todistus. Molemmat kohdat seuraavat suoraan Jacobin symbolin määritelmästä ja Legendren symbolin kertolaskun ominaisuuksista. □

Jacobin symbolilla on määritelty samat laskutoimituksiin liittyvät ominaisuudet kuin, mitkä on määritelty Legendren symbolille Määritelmässä 1.7. Koska Jacobin symboli on johdos Legendren symbolista, niin voidaan määritellä yleistetympi versio neliöjäännöksen käänteisyydestä seuraavan lauseen mukaisesti.

Lause 1.16. ***Yleistetty neliöjäännöksen käänteisyys*** *Parittomien ja positiivisten kokonaislukujen a ja b Jacobin symbolit voidaan määritellä seuraavasti:*

1. $\left(\frac{-1}{b}\right) = \begin{cases} 1, & jos\ b \equiv 1 \mod 4, \\ -1, & jos\ b \equiv 3 \mod 4. \end{cases}$

2. $\left(\frac{2}{b}\right) = \begin{cases} 1, & jos\ b \equiv 1 \ tai\ b \equiv 7 \mod 8, \\ -1, & jos\ b \equiv 3 \ tai\ b \equiv 5 \mod 8. \end{cases}$

3. $\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right), & jos\ a \equiv 1 \mod 4 \ tai\ b \equiv 1 \mod 4, \\ -\left(\frac{b}{a}\right), & jos\ a \equiv 3 \mod 4 \ ja\ b \equiv 3 \mod 4. \end{cases}$

Todistus. Sivuutetaan. □

Esimerkki 1.17. Onko luku 5417 neliöjäännös mod 8087?

Koska $5417 \equiv 1 \bmod 4$, voidaan Lauseen 1.16 kohdan 3 perusteella kääntää neliöjäännöllisyys, jolloin

$$\left(\frac{5417}{8087}\right) = \left(\frac{8087}{5417}\right) = \left(\frac{2670}{5417}\right).$$

Jaetaan Jacobin symbolin ominaisuuden 1.15 mukaan parillinen luku 2670 tekijöihin 2 ja 1335, josta seuraa

$$\left(\frac{2670}{5417}\right) = \left(\frac{2}{5417}\right)\left(\frac{1335}{5417}\right).$$

Koska $5417 \equiv 1 \bmod 8$ ja $\bmod 4$, niin Lauseen 1.16 kohtien 3 ja 2 perusteella voidaan kääntää neliöjäännös ja antaa luvulle 2 Jacobin symboliksi arvo 1 mod 5417, joten

$$\left(\frac{2}{5417}\right)\left(\frac{1335}{5417}\right) = 1 \cdot \left(\frac{5417}{1335}\right) = \left(\frac{77}{1335}\right).$$

Koska $77 \equiv 1 \bmod 4$, niin Lauseen 1.16 kohdan 3 mukaan voidaan kääntää neliöjäännöllisyys, niin

$$\left(\frac{77}{1335}\right) = \left(\frac{1335}{77}\right) = \left(\frac{26}{77}\right).$$

Jacobin symbolin ominaisuuden 1.15 nojalla voidaan jakaa parillinen luku 26 tekijöihin, jolloin

$$\left(\frac{26}{77}\right) = \left(\frac{2}{77}\right)\left(\frac{13}{77}\right).$$

Koska $77 \equiv 5 \bmod 8$ ja $77 \equiv 1 \bmod 4$, niin Lauseen 1.16 kohtien 2 ja 3 mukaan annetaan luvulle 2 Jacobin symbolin arvo -1 ja käännetään neliöjäännöllisyys, jolloin

$$\left(\frac{2}{77}\right)\left(\frac{13}{77}\right) = (-1)\cdot\left(\frac{77}{13}\right) = (-1)\cdot\left(\frac{12}{13}\right).$$

Lauseen 1.16 kohdan 1 mukaan, kun $13 \equiv 1 \bmod 4$ voidaan kääntää jäljelle jäänyt neliöjäännöllisyys, josta seuraa

$$(-1)\cdot\left(\frac{12}{13}\right) = (-1)\cdot 1 = -1.$$

Koska saatu Jacobin symboli on -1, niin luku 5417 on epäneliöjäännös mod 8087.

2 Neliöjäännösjärjestelmän käyttö salauksessa

Olkoon kokonaisluku $b = pq$ pariton ja kokonaisluku a neliöjäännös mod b. Jacobin symbolin nojalla voidaan merkitä, että $\left(\frac{a}{b}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1$. Voidaanko tästä päätellä a:n neliöjäännöllisyyttä p:n ja q:n suhteen?

Jaetaan tapaus kahteen tilanteeseen:

1.
$$\left(\frac{a}{b}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = (-1)\cdot(-1) = 1.$$

2.
$$\left(\frac{a}{b}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1\cdot 1 = 1.$$

Huomataan, että ainoa tieto mitä saadaan selville on, että a ei voi olla pelkästään toisen p:n tai q:n kanssa epäneliöjäännös. Mitään tarkkaa tietoa a:n neliöjäännöllisyydestä p:n tai q:n suhteen ei siis saada, jos tiedetään vain a:n neliöjäännöllisyys b:n suhteen. Tätä tietoa voidaan käyttää kryptografiassa hyväksi.

Tässä tutkielmassa tutustutaan probalistiseen Goldwasser-Micalin salausjärjestelmään, joka käyttää hyväksi aikaisemmin mainittua neliöjäännöksen ominaisuutta.

2.1 Probalistiseen Goldwasser-Micalin salaus

Viestin vastaanottaja valitsee kaksi suurta salaista alkulukua p ja q, joiden avulla hän valitsee luvun a siten, että $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = -1$. Vastaanottaja julkistaa arvot $N = pq$ ja a.

Viestin lähettäjä salaa jokaisen viestin yksittäisen bitin $m \in [0,1]$ satunnaisesti valittavan r:n, $r \in \mathbb{Z}$ avulla, joka valitaan jokaiselle bitille erikseen väliltä $1 < r < N$. Varsinainen salaus tapahtuu seuraavalla tavalla:

$$c = \begin{cases} r^2 \mod N, & \text{jos } m = 0, \\ ar^2 \mod N, & \text{jos } m = 1. \end{cases}$$

Viestin lähettäjä lähettää salatun viestin c vastaanottajalle. Vastaanottaja avaa salatun viestin c tutkimalla c:n salattujen bittien neliöjäännöllisyyttä mod p suhteen seuraavasti:

$$m = \begin{cases} 0, & \text{jos } \left(\frac{c}{p}\right) = 1, \\ 1, & \text{jos } \left(\frac{c}{p}\right) = -1. \end{cases}$$

Tarkistetaan lyhyesti, että salatut bitit avautuvat oikein, kun käytetään edellistä avaamistapaa.

$$\left(\frac{c}{p}\right) = \begin{cases} \left(\frac{r^2}{p}\right) = \left(\frac{r}{p}\right)\left(\frac{r}{p}\right) = \left(\frac{r}{p}\right)^2 = 1, & \text{jos } m = 0, \\ \left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{r}{p}\right)^2 = \left(\frac{a}{p}\right) = -1, & \text{jos } m = 1. \end{cases}$$

Huomataan, että viestin yksittäiset bitit salautuvat ja avautuvat oikein, mutta entä, jos salausta yritetään avata julkisella avaimella N ilman, että tiedetään tekijöihinjakoa $n = pq$:

$$\left(\frac{c}{N}\right) = \begin{cases} \left(\frac{r^2}{N}\right) = \left(\frac{r}{N}\right)\left(\frac{r}{N}\right) = \left(\frac{r}{N}\right)^2 = 1, & \text{jos } m = 0, \\ \left(\frac{ar^2}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{r}{N}\right)^2 = \left(\frac{a}{q}\right)\left(\frac{a}{p}\right) = (-1)\cdot(-1) = 1, & \text{jos } m = 1. \end{cases}$$

Huomataan, että riippumatta r:n ja a:n arvoista, kun yritetään avata salattua bittiä julkisella avaimella N saadaan aina Jacobin symbolin arvoksi luku 1.
Nimitys probabilistinen salaus tulee satunnaisesta r:n valitsemisesta, jonka seurauksena jokainen salattu bitti on satunnainen kokonaisluku välillä $1 < c < N$.

Huomautus 2.1. Lauseessa 1.5 todettiin, että todennäköisyys sille, että satunnaisesti valittu luku on epäneliöjäännös on 50%. Todennäköisyys sille, että satunnaisesti valittu luku on neliöjäännös kahden erisuuruisen parittoman alkuluvun suhteen on 25%. Tämä ei silti tarkoita, että jokaiselle alkulukuparille löytyisi yhteinen epäneliöjäännös. Esimerkiksi alkuluvuilla 11 ja 311 ei ole olemassa yhtään yhteistä epäneliöjäännöstä.

Esimerkki 2.2. Vastaanottaja valitsee salaiset avaimet $p = 71$ ja $q = 83$. Vastaanottaja kokeilee onko arvo $a = 34$ epäneliöjäännös mod 71 ja mod 83.

Tarkastetaan, onko luku 34 epäneliöjäännös mod 71.
Jaetaan luku 34 tekijöihin Jacobin symbolin ominaisuuksien mukaan, jolloin

$$\left(\frac{34}{71}\right) = \left(\frac{2}{71}\right)\left(\frac{17}{71}\right).$$

Koska $71 \equiv 3 \bmod 4$ ja $17 \equiv 1 \bmod 8$, niin luvun 2 Jacobin symboli on 1 ja jäljelle jäänyt neliöjäännös voidaan kääntää, josta seuraa

$$\left(\frac{2}{71}\right)\left(\frac{17}{71}\right) = \left(\frac{71}{17}\right) = \left(\frac{3}{17}\right).$$

Jäljelle jäänyt neliöjäännös voidaan kääntää uudelleen sillä, $17 \equiv 1 \bmod 4$ ja luvun 2 Jacobin symboli saa arvon -1 sillä $3 \equiv 3 \bmod 8$, jolloin

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Tarkastetaanko onko luku 34 neliöjäännös mod 83.
Jaetaan luku 34 tekijöihin Jacobin symbolin ominaisuuksien mukaan, jolloin

$$\left(\frac{34}{83}\right) = \left(\frac{17}{83}\right)\left(\frac{2}{83}\right).$$

Koska luku $17 \equiv 1 \bmod 4$, neliöjäännös voidaan kääntää ja luku 2 saa Jacobin symbolin arvon -1, koska $83 \equiv 3 \bmod 8$, niin

$$\left(\frac{17}{83}\right)\left(\frac{2}{83}\right) = \left(\frac{83}{17}\right)\cdot(-1) = \left(\frac{15}{17}\right)\cdot(-1).$$

Neliöjäännös voidaan kääntää, koska $17 \equiv 1 \bmod 4$ ja, koska $15 \equiv 7 \bmod 8$ luvun 2 Jacobin symboli on 1, josta seuraa

$$\left(\frac{15}{17}\right)\cdot(-1) = \left(\frac{17}{15}\right)\cdot(-1) = \left(\frac{2}{15}\right)\cdot(-1) = (1)\cdot(-1) = -1.$$

Luku 34 on epäneliöjäännös mod 83 ja mod 71. Vastaanottaja laskee $N = 71 \cdot 83 = 5893$ ja julkaisee julkiset avaimet $a = 34$ ja $N = 5893$.

Viestin lähettäjä haluaa lähettää viestin $m = 10$. Lähettäjä valitsee $r = 93$ ja, koska $m_1 = 1$, niin hän laskee:

$$c_1 \equiv r^2 a \equiv 93^2 \cdot 34 \equiv 8683 \equiv 2790 \bmod 5893.$$

Toiseksi r:n arvoksi hän valitsee $r = 113$ ja laskee, koska $m_2 = 0$, niin

$$c_2 \equiv r^2 \equiv 113^2 \equiv 12769 \equiv 983 \bmod 5893.$$

Lähettäjä lähettää viestit $c_1 = 2790$ ja $c_2 = 983$ vastaanottajalle.

Vastaanottaja saa viestit $c_1 = 2790$ ja $c_2 = 983$, jonka jälkeen hän tutkii saatujen lukujen neliöjäännöllisyyttä mod 71 suhteen.

Tutkitaan aluksi luvun $c_1 = 2790$ neliöjäännöllisyyttä mod 71 suhteen. Jaetaan luku 21 tekijöihin Jacobin symbolin ominaisuuksien mukaan, jolloin

$$\left(\frac{c_1}{p}\right) = \left(\frac{2790}{71}\right) = \left(\frac{21}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{7}{71}\right).$$

Koska $3, 7, 71 \equiv 3 \bmod 4$, niin neliöjäännökset voidaan kääntää ja muutetaan ne negatiivisiksi, josta seuraa

$$\left(\frac{3}{71}\right)\left(\frac{7}{71}\right) = -\left(\frac{71}{3}\right)\left(-\left(\frac{71}{7}\right)\right).$$

Luku 1 on selvästi neliöjäännös mod 7 ja, koska $3 \equiv 3 \bmod 4$, niin luvun 2 Jacobin symboli on -1, jolloin

$$-\left(\frac{71}{3}\right)\left(-\left(\frac{71}{7}\right)\right) = -\left(\frac{2}{3}\right)\left(-\left(\frac{1}{7}\right)\right) = -1.$$

Koska $c_1 = 2790$ on epäneliöjäännös mod 71, niin $m_1 = 1$.

Tutkitaan luvun $c_2 = 983$ neliöjäännöllisyyttä mod 71 suhteen. Jaetaan luku 60 tekijöihin Jacobin symbolin ominaisuuksien mukaan. Koska $15, 71 \equiv 3 \bmod 4$, niin neliöjäännös voidaan kääntää ja muuttaa negatiiviseksi, jolloin

$$\left(\frac{c_2}{p}\right) = \left(\frac{983}{71}\right) = \left(\frac{60}{71}\right) = \left(\frac{2}{71}\right)^2 \cdot \left(\frac{15}{71}\right) = -\left(\frac{71}{15}\right).$$

Neliöjäännös voidaan kääntää ja muuttaa negatiiviseksi, koska $11, 15 \equiv 3 \bmod 4$, josta seuraa

$$-\left(\frac{71}{15}\right) = -\left(\frac{11}{15}\right) = \left(\frac{15}{11}\right).$$

Jacobin symbolin ominaisuuksien mukaan voidaan jakaa luku 4 tekijöihin, niin

$$\left(\frac{15}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{2}{11}\right)^2 = 1.$$

Koska luku $c_2 = 983$ on neliöjäännös mod 71, niin $m_2 = 0$.
Vastaanotettiin siis viesti $m = 10$.

2.2 Rabinin allekirjoitusjärjestelmä

Rabinin allekirjoitujärjestelmä perustuu muotoa $p = 4k-1,\ k \in \mathbb{Z}$ olevien alkulukujen ominaisuuteen, joka mahdollistaa nopean neliöjäännöksen juuren laskemisen.

Merkinnällä $\sqrt{m}$ tarkoitetaan toista arvoista $x = c$ tai $x = -c$, jotka toteuttavat $x^2 \equiv m \bmod n$ ja merkinnällä m^{-1} merkitään luvun m käänteisalkiota jäännösluokassa mod n.

Tässä kappaleessa on käytetty pääasiallisena lähteenä Michael O. Rabinin julkaisua Digitalized Signatures and Public Key Functions as Intractable as Factorization [3].

Lause 2.3. *Olkoon luku p pariton alkuluku ja muotoa $p = 4k - 1$, jossa $k \in \mathbb{Z}$ ja olkoon luku m neliöjäännös mod p. Tästä seuraa, että $\sqrt{m}$ saadaan laskettua nopeasti käyttäen seuraavaa laskutapaa.*

$$m^{\frac{p+1}{4}} \equiv \sqrt{m} \ mod \ p.$$

Toinen arvoista $\sqrt{m}$ saadaan laskettua vähentämällä saatu arvo moduloluvusta.

Todistus. Lauseen 1.9 perusteella, jos luku m on neliöjäännös mod p niin se voidaan esittää seuraavassa muodossa:

$$m^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Kerrotaan yhtälö puolittain luvulla m, jolloin

$$m^{\frac{p-1}{2}} \cdot m \equiv m^{\frac{p+1}{2}} \equiv m \bmod p.$$

Korotetaan saatu lauseke puolittain luvulla $\frac{1}{2}$, jolloin

$$m^{\frac{p+1}{4}} \equiv m^{\frac{1}{2}} \equiv \sqrt{m} \bmod p.$$

□

Esimerkki 2.4. Mikä on luvun m arvo, kun $m^2 \equiv 13 \bmod 23$?
Koska $23 = 4 \cdot 6 - 1$, niin voidaan käyttää ratkaisemiseen Lausetta 2.3, josta seuraa

$$\sqrt{13} \equiv 13^{\frac{23+1}{4}} \equiv 13^6 \equiv 8^3 \equiv 512 \equiv 6 \bmod 23.$$

Tällöin $m = 6$ tai $m = 23 - 6 = 17$.

Seuraavassa hash-funktion määritelmässä on käytetty lähteenä Phillip Rogaway ja Thomas Shrimpton julkaisua liittyen hash-funktioihoin [4].

Määritelmä 2.5. Hash-funktio on funktio, joka tuottaa annetulle lähtöjoukon arvolle satunnaiselta näyttävän maalijoukon arvon. Hash-funktion pitää toteuttaa seuraavat kolme ominaisuutta.

1. Hash-funktion S maalijoukon arvoista x on äärimmäisen vaikea laskea lähtöjoukon vastaavia alkioita.

2. Jos tiedetään luvun y_1 hash-funktion arvo $S(y_1) = x$, on äärimmäisen vaikea etsiä toista lukua y_2, joka kuvautuu $S(y_2) = x$, kun $y_1 \neq y_2$.

3. On vaikea löytää kaksi alkiota y_1 ja y_2, jotka tuottavat samat arvot hash-funktiolla S.

Lause 2.6. *Olkoon parittomat alkuluvut p ja q muotoa $p = 4k - 1$ ja $q = 4j - 1$, joissa $j, k \in \mathbb{Z}$. Luku $n = pq$ on tällöin muotoa $n = 4v + 1$, jossa $v = (4kl - k - l)$ ja $v \in \mathbb{Z}$.*

Todistus. Käytetään edellisen lauseen mukaan määriteltyjä arvoja luvuille p, q ja n, jolloin

$$n = pq = (4k - 1)(4j - 1) = 16kl - 4k - 4l + 1 = 4(4kl - k - l) + 1.$$

□

Huomautus 2.7. Jos luku n ei ole muotoa $n = 4v - 1$ $v \in \mathbb{Z}$, Lausetta 2.3 ei voida käyttää neliöjäännöksien juurien määrittämiseen mod n, jolloin kyseisten juurien määrittäminen on hidasta. Lisäksi, jos tiedetään yhdistetyn luvun tekijöihin jako $n = pq$, niin neliöjäännöksien juuret voidaan etsiä aluksi mod p ja mod q suhteen, jonka jälkeen kyseiset neliöjäännökset saadaan mod n suhteen alla olevasta yhtälöparista käyttäen Kiinalaista jäännöslausetta:

$$x \equiv x_p + t \cdot p \bmod n, \text{ jossa } t \in \mathbb{Z},$$

$$x \equiv x_q + h \cdot q \bmod n, \text{ jossa } h \in \mathbb{Z}.$$

Edellisellä lauseella saadaan laskettua yksi sopiva x:n arvo neljästä muusta mahdollisesta. Muut x:n arvot saadaan laskettua käyttäen eri kombinaatiota modulo p juurista x_p ja modulo q juurista x_q, jotka on laskettu Lausetta 2.3 käyttäen.

Aikaisempien lauseiden perusteella *Rabinin allekirjoitusjärjelmä* määritellään seuraavasti. Allekirjoittaja valitsee kaksi suurta alkulukua p ja q, jotka ovat muotoa $p, q \equiv 3 \bmod 4$. Sen lisäksi allekirjoittaja laskee luvun $n = pq$,

valitsee luvun b väliltä $0 \leqslant b < n$ ja julkaisee parin (n, b). Viestiä allekirjoittaessaan allekirjoittaja lisää kokonaisen salatun viestin M loppuun satunnaisesti valitun lisäsanan U, jonka pituus $L(U) = k$ on sovittu aiemmin viestin vastaanottajan kanssa. Tämän lisäksi allekirjoittaja laskee julkisella hash-funktiolla S salatun viestin ja allekirjoituksen yhdistetyn arvon $S(MU) \equiv h \bmod n$. Seuraavaksi allekirjoittaja tutkii, millä x:n arvolla yhtälö $x(x + b) \equiv h \bmod n$ toteutuu.

Muokataan yhtälö helpommin ratkaistavaan muotoon käyttäen potenssilaskun ominaisuuksia seuraavasti

$$x(x + b) \equiv h \bmod n$$

$$x^2 + xb \equiv h \bmod n$$

$$x^2 + xb + 4^{-1} \cdot b^2 - 4^{-1} \cdot b^2 \equiv h \bmod n$$

$$\left(x + 2^{-1} \cdot b\right)^2 \equiv h + 4^{-1} \cdot b^2 \bmod n.$$

Nyt ongelma ollaan saatu muotoiltua muotoon: Onko luku $(h + 4^{-1} \cdot b^2)$ neliöjäännös mod n. Seurauksen 2.7 mukaan voidaan neliöjäännöllisyys tutkia aluksi luvun n tekijöiden suhteen. Jos kyseinen arvo ei ole neliöjäänös mod p ja mod q suhteen valitaan uusi U ja lasketaan uusi hash-funktion arvo viestille M ja lisäykselle U. Kun on löydetty sopiva lisäys U, lasketaan $\sqrt{h + 4^{-1} \cdot b^2}$ mod p ja mod q suhteen Lauseen 2.3 avulla. Saaduista arvoista saadaan laskettua x:n arvot mod p ja mod q suhteen, joista saadaan laskettua x:n arvo mod n suhteen seurauksen 2.7 avulla.

Tämän jälkeen allekirjoittaja lähettää salatun viestin M, jonka mukana viestin allekirjoitus-parin (U, x) vastaanottajalle. Kuka tahansa voi varmistaa allekirjoittajan oikeaksi laskemalla julkisen hash-funktion arvon $S(MU)$ mod n ja vertaamalla sen arvoa arvoon $x(x+b)$ mod n. Lisäksi pitää tarkastaa, että lisäys U on sovitun mittainen.

Esimerkki 2.8. Tässä esimerkissä on käytetty pythonin hashlib-kirjaston sha1 hash-funktiota. Olkoon $p = 11$, $q = 19$, $n = 209$ ja $b = 31$. Viestin lähettäjä julkaisee julkiset avaimet $(n, b) = (209, 31)$. Allekirjoittaja haluaa allekirjoittaa ja lähettää salaisen viestin $M = 37$. Lisäyksen pituudeksi on sovittu vastaanottajan kanssa $L(U) = 2$, joten lähettäjä valitsee arvon $U = 29$. Tällöin käyttäen julkista hash-funktiota saadaan salatulle viestille ja sen lisäykselle arvo $S(MU) \equiv h \equiv S(3729) \equiv 21344 \equiv 26 \bmod 209$. Nyt lähettäjä tutkii onko luku $h + 4^{-1} \cdot b^2 \equiv 26 + 4^{-1} \cdot 31^2 \equiv 26 + 4^{-1} \cdot 125 \equiv 5 \bmod 209$

neliöjäännös mod 19 ja mod 11 suhteen.

Koska $5 \equiv 1 \bmod 4$, voidaan kääntää neliöjäännös Lauseen 1.16 mukaan molemmissa kohdissa, jolloin

$$\left(\frac{h + 4^{-1} \cdot b^2}{q}\right) = \left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1,$$
$$\left(\frac{h + 4^{-1} \cdot b^2}{p}\right) = \left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Koska luku 5 on neliöjäännös mod 19 ja mod 11 etsitään arvo $\sqrt{5}$ käyttäen Lausetta 2.3 seuraavasti:

$$\sqrt{m} \equiv m^{\frac{p+1}{4}} \equiv 5^{\frac{11+1}{4}} \equiv 5^3 \equiv 125 \equiv 4 \bmod 11$$

$$\sqrt{m} \equiv m^{\frac{q+1}{4}} \equiv 5^{\frac{20}{4}} \equiv 5^5 \equiv 3125 \equiv 9 \bmod 19.$$

Seuraavaksi ratkaistaan lausekkeesta $x + 2^{-1} \cdot b \equiv \sqrt{m}$ x:n arvo p:n suhteen, jolloin

$$x_{11} + 2^{-1} \cdot 31 \equiv 4 \bmod 11$$
$$x_{11} + 10 \equiv 4 \bmod 11$$
$$x_{11} \equiv -6 \bmod 11$$
$$x_{11} \equiv 5 \bmod 11.$$

Ratkaistaan lausekkeesta $x + 2^{-1} \cdot b \equiv \sqrt{m}$ x:n arvo myös q:n suhteen, jolloin

$$x_{19} + 2^{-1} \cdot 31 \equiv 9 \bmod 19$$

$$x_{19} + 6 \equiv 9 \bmod 19$$
$$x_{19} \equiv 3 \bmod 19.$$

Käytetään Kiinalaista jäännöslausetta saaduilla arvoilla huomautuksen 2.7 mukaisesti, jolloin

$$x \equiv 5 + 11 \cdot t \bmod 209 \text{ ja}$$
$$x \equiv 3 + 19 \cdot h \bmod 209.$$

Merkitään yllä olevat lauseet yhtä suuriksi, jolloin saadaan

$$5 + 11 \cdot t \equiv 3 + 19 \cdot h \bmod 209.$$

Kerrottaessa saatu yhtälö luvulla 19, jolloin luvun t kertoimeksi saadaan $209 \equiv 0 \bmod 209$, jolloin

$$38 \equiv 152 \cdot h \bmod 209.$$

Saadusta yhtälöstä ratkaistaan seuraava h:n arvo:

$$h \equiv 3 \bmod 209.$$

Seuraavaksi sijoitetaan arvo $h \equiv 3 \bmod 209$ alun yhtälöön, jolloin saadaan

$$x \equiv 3 + 19 \cdot 3 \equiv 60 \bmod 209.$$

Lähettäjä allekirjoittaa salatun viestin $M = 37$ parilla $(U, x) = (29, 60)$ ja lähettää viestin ja allekirjoituksen vastaanottajalle. Vastaanottaja käyttää julkisesti tiedettyä hash-funktiota S laskeakseen viestin ja lisäyksen arvon $S(MU) = 21344 = 26 \bmod 209$ ja vertaa saatua arvoa arvoon $x(x + b) \equiv 60(60 + 31) \equiv 5460 \equiv 26 \bmod 209$. Lisäksi lisäyksen $U = 29$ pituus on oikea sillä $L(U) = 2$. Koska arvot täsmäsivät ja lisäyksen U pituus oli oikea, voidaan olla varmoja, että viesti on oikealta lähettäjältä.

Lähdeluettelo

[1] Jeffrey Hoffstein, Jill Pipher ja Joseph H. Silverman, An Introduction to Mathematical Cryptography, Springer Science+Business Media LLC, 2008

[2] Katre, S., Rajwade, A., Euler's Criterion for Quintic Nonresidues, Can. J. Math., Vol. XXXVII, No. 5, 1985, pp. 1008-1024, Canadian Journal of Mathematics, 1985

[3] Michael O. Rabin, Digitalized Signatures and Public Key Functions as Intractable as Factorization, Massachusetts institute of technology laboratory for computer science, 1979

[4] Rogaway P., Shrimpton T. Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In: Roy B., Meier W. (eds) Fast Software Encryption. FSE 2004. Lecture Notes in Computer Science, vol 3017, pp. 371-388. Springer, Berlin, Heidelberg, 2004